Threat Brief: Hancitor Actors

By Unit 42

Published: 2018-02-07 · Archived: 2026-04-02 11:18:04 UTC

If you need to understand one thing about cybercrime, it's that it is all about business.

In our latest Unit 42 research on cybercriminals using the Hancitor malware, we show that not only are their attacks about business, we can see these cybercriminals deftly applying some fundamental business principles around timing, specialization, and globalization.

Hancitor is a malware that focuses getting other malware onto the victim's system. In the case of Hancitor, it's typically banking Trojans that steal the victim's banking information.

In our latest research, we can see the attackers behind Hancitor have been timing their attacks to happen during the busiest time of the global working week, the middle of the week. And we've seen that in adapting their attacks to better evade detection, they've specialized their operations around the globe.

Hancitor isn't particularly advanced in its tactics: it's ideal target is an old or outdated version of Microsoft Windows like Windows 7 or even Windows XP. But it's effective enough that when used in several hundred different spam campaigns every month it pays for the criminals to keep up these attacks against targets around the world.

Timing

In our most recent research, one of the things that jumped out for our researchers is the clear pattern around the timing of the attacks. As you can see in Figure 1 below, throughout 2017, the Hancitor attacks show clear spikes in their occurrence and these spikes happen during the middle of the week.

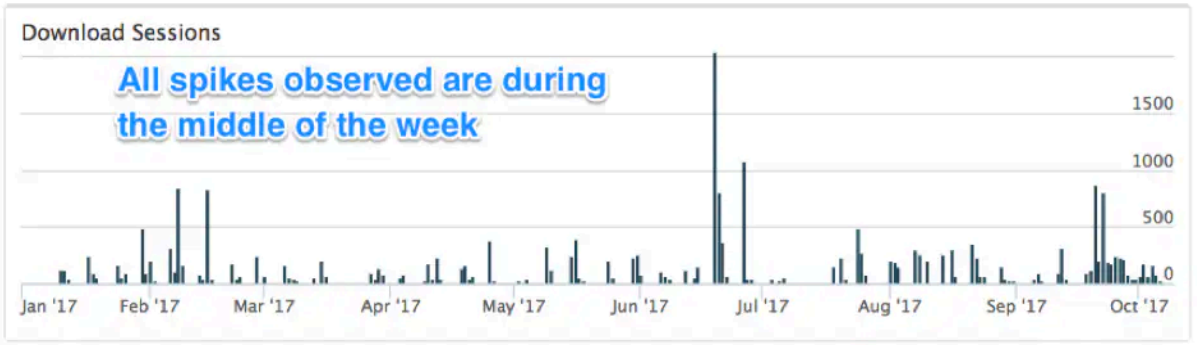

Figure 1: Timeline of Hancitor campaign activity since January 2017.

The attackers behind Hancitor aren't the first to time their spam attacks like this, but it is an effective tactic to try and increase their chances of success, especially when combined with the other innovation that we've seen.

Adapting the Attacks

In the past, Hancitor was sent as a malicious attachment in a spam email which would then download and install the attackers' final malware like a banking Trojan. When they would do this, the Hancitor attachment would download and install the final malware from a malicious or compromised site.

But as organizations have gotten more effective at blocking malicious attachments like Hancitor, we've seen the attackers behind Hancitor adapt to evade detection and prevention.

They've done this by moving the Hancitor malware from being a malicious attachment in spam to itself being a malicious download. The spam the attackers use no long has a malicious attachment but instead a malicious link that downloads the malicious Hancitor attachment.

To do this, they make the spam look like something that requires you to click and download something like and invoice, a message, or a delivery notification. Figure 2 shows one of these that was made to look like an Amazon shipping notice.

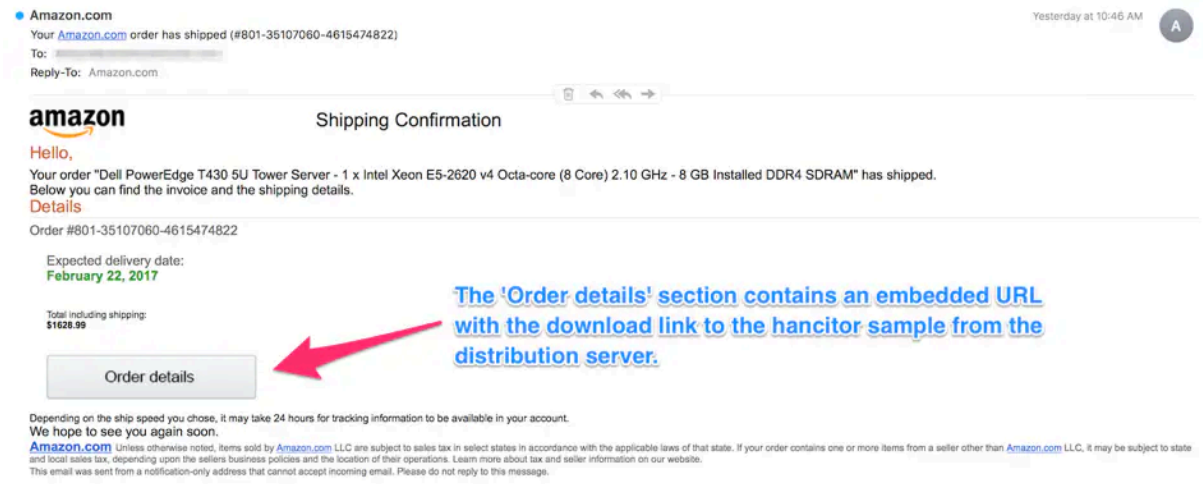

Figure 2: Hancitor malspam example from February 2017.

This means that a Hancitor attack now has two downloads rather than one and what these attackers did around the malicious downloads shows another modern business tactic: globalization.

Globalizing the Attacks

Figure 3 below is a map showing where our Unit 42 researchers have found webistes involved in Hancitor attacks.

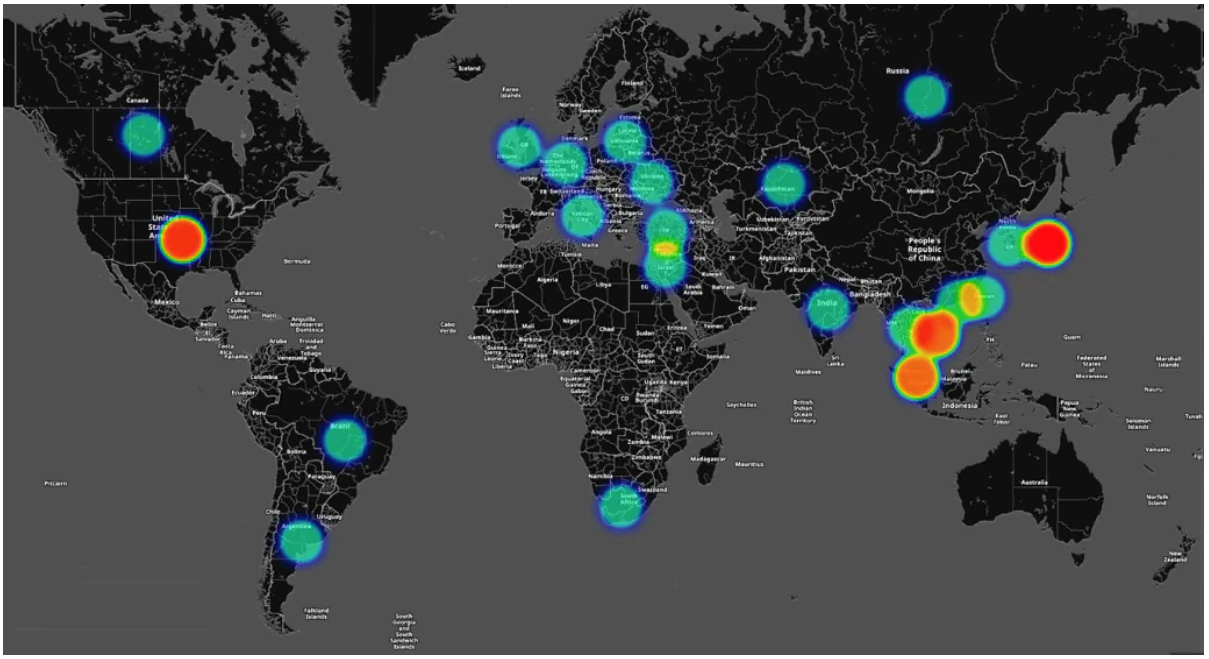

Figure 3: Hancitor distribution servers globally thus far in 2017

Country	Number of Distribution servers
United States	197
Japan	23
Vietnam	13
Singapore	12
Russia	7
Brazil	6
Malaysia	6
Hong Kong	5
South Africa	4
Thailand	4
India	2
Ireland	2
Kazakhstan	2
Taiwan	2
Turkey	2

Ukraine	2
Argentina	1
Canada	1
Germany	1
Israel	1
Italy	1
Netherlands	1
Republic of Korea	1
Republic of Lithuania	1
United Kingdom	1

Table 1 – Number of Distribution Servers by Country

The hot spots in the United States represents distribution servers which are created using fraud based accounts at various hosting providers that are hosting the Hancitor documents while the hotspots in Asia represent legitimate sites for small and medium businesses that have been compromised by the actors behind Hancitor campaign to host the malicious Hancitor documents.

Conclusion

Attackers are always making business decisions to optimize their attacks in ways that are most successful and profitable. What is most interesting about Hancitor is the way these decisions so clearly reflect an awareness of business realities (by targeting peak working times) and dividing up the “work” of their attacks in a way that so clearly mirrors mainstream business decisions around globalizing operations.

In the end, while Hancitor may not be sophisticated, these steps to adapt and stay effective seem to be succeeding. And we expect to continue to see Hancitor be a global threat for the foreseeable future.
